AMENDMENT TO THE CLAIMS

A listing of the claims presented in this patent application appears below. This listing replaces all prior versions and listing of claims in this patent application.

1. (currently amended) A storage device comprising:

a storage medium for retaining data; and

a cryptographic processing unit which receives, from a host device, and executes a command corresponding to each of the plurality of sequenced subprocesses produced by dividing each of a ~~plurality of commands from a host device to execute the commands upon performing a plurality of~~ series of cryptographic input[[/]] and output ~~processing~~ processes for encrypting data to be secured and inputting[[/]] and outputting the data between the storage medium and [[a]] the host device, ~~the commands being issued by dividing the plurality of series of cryptographic input/output processing each into a plurality of procedures~~[[,]]

wherein the cryptographic processing unit simultaneously processes subprocesses respectively belonging to two or more different cryptographic input and output processes by ~~refers~~ referring to identifying information attached to the command and ~~to identify~~ identifying to which cryptographic input[[/]] and output ~~processing~~ process the command belongs ~~to, then simultaneously performing two or more of the plurality of cryptographic input/output processing procedures~~.

2. (currently amended) The storage device according to claim 1, wherein the cryptographic processing unit manages the sequence of commands executed in each cryptographic input[[/]] and output ~~processing~~ process and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command.

3. (currently amended) The storage device according to claim 2, wherein when the cryptographic processing unit receives the incorrectly sequenced command, the cryptographic processing unit interrupts the cryptographic input[[/]] and output ~~processing~~ process to which the command belongs.

4. (currently amended) The storage device according to claim 1, wherein the number of the cryptographic input[[/]] and output ~~processing~~ processes which can be performed simultaneously by the storage device is predetermined in accordance with a performance of the storage device.

5. (currently amended) The storage device according to claim 1, wherein in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input[[/]] and output ~~processing~~ processes which can be performed simultaneously by the storage device.

6. (original) The storage device according to claim 1, wherein the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data to be exchanged bypassing the cryptographic processing unit, the confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit.

7. (currently amended) A storage device comprising:

a storage medium for retaining data; and

a cryptographic processing unit for receiving, from a host device, and executing a command corresponding to each of the plurality of sequenced subprocesses produced by dividing each of a ~~plurality of commands from a host device to execute the commands upon performing a~~ series of cryptographic input[[/]] and output ~~processing~~ processes for encrypting data to be secured and inputting[[/]] and outputting the data between the storage medium and the host device, ~~the commands being issued by dividing the series of cryptographic input/output processing into a plurality of procedures~~[[,]]

wherein the cryptographic processing unit simultaneously processes subprocesses respectively belonging to two or more different cryptographic input and output processes by ~~can manage two or more cryptographic input/output processings, and refer~~ referring to identifying information attached to the command [[to]] and ~~identify~~ identifying to which cryptographic input[[/]] and output ~~processing~~ process the received command belongs [[to]], and rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input[[/]] and output ~~processing~~ process to which the command belongs.

8. (currently amended) The storage device according to claim 7, wherein in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input[[/]] and output ~~processing~~ processes which can be performed simultaneously by the storage device.

9. (original) The storage device according to claim 7, wherein the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data to be exchanged bypassing the cryptographic processing unit, the confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit.

10. (currently amended) A host device which exchanges data with a storage device that is capable of simultaneously performing a plurality of series of input[[/]] and output ~~processing~~ processes for encrypting data to be secured and inputting[[/]] and outputting the data, the host device comprising:

a controller which divides the cryptographic input[[/]] and output ~~processing~~ processes into a plurality of sequenced subprocesses ~~procedures~~ and ~~issuing~~ issues commands sequentially to the storage device thereby allowing the storage device to ~~in order to make the storage device~~ execute a ~~procedure~~ subprocess to be executed on the storage-device side; and

a cryptographic processing unit which carries out encryption or decryption that is required of the cryptographic input[[/]] and output ~~processing~~ process,

wherein when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input[[/]] and output ~~processing~~ processes the command belongs.

11 (currently amended). The host device according to claim 10, wherein the controller issues a command to allocate a process system for performing the cryptographic input[[/]] and output ~~processing~~ process prior to initiation of the cryptographic input[[/]] and output ~~processing~~ process.

12 (currently amended). A data input[[/]] and output method, when performing cryptographic input[[/]] and output ~~processing~~ process between a host device and a storage device that is capable of simultaneously performing a plurality of series of cryptographic input[[/]] and output ~~processing~~ processes for encrypting data to be secured and inputting[[/]] and outputting the data, and storing data to be exchanged through the cryptographic input[[/]] and output ~~processing~~ process, comprising:

dividing the cryptographic input[[/]] and output ~~processing~~ processes divided into a plurality of procedures and allowing the host device to execute a procedure to be executed on the host-device side out of the procedures;

allowing the host device to issue a command to the storage device in order to make the storage device execute a procedure to be executed on the storage-device side;

allowing the storage device to receive the command; and

allowing the storage device to execute the command,

wherein identifying information is attached to the command to identify to which one of the plurality of cryptographic input[[/]] and output ~~processing~~ processes, being performed simultaneously by the storage device, the command belongs.

13 (currently amended). The data input[[/]] and output method according to claim 12, further comprising predetermining an upper-limit number of the cryptographic input[[/]] and output ~~processing~~ processes that can be performed simultaneously by the storage device in accordance with performance of the storage device.

14 (currently amended). The data input/output method according to claim 12, further comprising:

allowing the storage device to predetermine an upper-limit number of the cryptographic input[[/]] and output ~~processing~~ processes that the storage device can perform simultaneously in accordance with its own performance, and

informing the host device of the upper limit.

15 (currently amended). The data input[[/]] and output method according to claim 13, further comprising, prior to performing the cryptographic input[[/]] and output ~~processing~~ processes, selecting and allocating identifying information for identifying the cryptographic input[[/]] and output ~~processing~~ process to be performed from among the prepared number of pieces of identifying information determined in the determining step.

16 (currently amended). The data input[[/]] and output method according to claim 14, further comprising, prior to performing the cryptographic input[[/]] and output ~~processing~~ processes, selecting and allocating identifying information for identifying the cryptographic input[[/]] and output ~~processing~~ process to be performed from among the prepared number of pieces of identifying information determined in the determining step.

17 (currently amended). The data input[[/]] and output method according to claim 12, wherein the receiving step comprises:

determining whether the received command is a correctly sequenced command in the cryptographic input[[/]] and output ~~processing~~ process;

accepting the command successfully when the received command has been determined to be a correctly sequenced command; and

rejecting the execution of the received command when the received command has been determined to be an incorrectly sequenced command.

18. (currently amended). The data input[[/]] and output method according to claim 17, wherein when the received command has been determined to be an incorrectly sequenced command, the execution of the cryptographic input[[/]] and output ~~processing~~ process to which the command belongs is interrupted.